REMARKS/ARGUMENTS

Claims 1-23 are pending in the present application. Claims 1, 9, 16, and 23 are amended. Support for the amendments may be found at least in the Specification at least on page 2, lines 7-28, Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 102, Anticipation

The Examiner rejected claims 1, 5, 7-9, 13, 15, 16, 20, 22 and 23 under 35 U.S.C. § 102(b) as anticipated by *Garrison*, System and Method for Restricting Unauthorized Access to a Database, U.S. Patent No. 6,385,730, dated May 7, 2002 (hereinafter referred to as "*Garrison*"). This rejection is respectfully traversed.

Applicants first address this rejection with respect to claim 1. In rejecting claim 1, the Examiner states the following:

> Claims 1, 5, 7-9, 13, 15, 16, 20, 22, 23 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by U. S. Patent No. 6,385,730 to Garrison. As per claims 1, 5, 7-9, 13, 15, 16, 20, 22 and 23, Garrison discloses the limitations of these claims (see at least the abstract and fig. 4A).

Office Action dated June 26, 2007, p.2

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). In this case, each and every feature of the presently claimed invention is not identically shown in the cited reference, arranged as they are in the claims.

Amended claim 1 is as follows:

> 1. (Currently Amended) A method in a first server data processing system for responding to a denial of service attack from a client, the method comprising:
>
> detecting an occurrence of the denial of service attack from the client in which credentials are presented to the first server data processing system by the client, wherein the denial of service attack comprises sending invalid credentials to a server to consume resources of the server;
>
> responsive to detecting the occurrence of the denial of service attack, blocking connections from the client to the first server data processing system,;

responsive to detecting the occurrence of the denial of service attack, replaying an instance of the denial of service attack to a second server data processing system; and

responsive to a failure of the instance of the denial of service attack on the second server data processing system, sending a command to the second server data processing system to block connections from the client.

I.A. Garrison Fails to Disclose Blocking Connections from the Client to the First Server Data Processing System in Response to Detecting an Occurrence of the Denial of Service Attack from the Client in which Credentials are Presented to the First Server Data Processing System by the Client.

Garrison fails to anticipate amended claim 1, because *Garrison* is devoid of disclosure of the first two steps of claim 1. *Garrison* does not disclose the features of blocking connections from the client to the first server data processing system in response to detecting an occurrence of the denial of service attack from the client in which credentials are presented to the first server data processing system by the client.

In rejecting claim 1, the Examiner cites to *Garrison* at the abstract which states the following:

> A secure client/server system provides remote access to a database system without allowing unauthorized users to access data stored within the database system. A client computer (client) establishes communication with server computer (server) and transmits a user password to the server. The server receives the user password and translates the user password into an alias or different password. When the client submits a request for data contained in the database system, the server accesses a database system associated with the server using the alias password. The database system allows the server to access information within the database system based on the alias password. Since the database system recognizes the alias password instead of the user password, only attempts to access the database via the server (after passing the security measures in place at the server) should be successful.

The cited portion discloses a client/server system that focuses on providing remote access to a database system without allowing unauthorized users to access data stored within the database system. *Garrison* discloses the process of transmitting and translating an **alias password** to either grant or deny access to a user. However, *Garrison* does not address the problem of responding to a denial of service attack in which invalid credentials are sent to a server to consume resources of the server. In fact, *Garrison* does not even acknowledge that the problem exists, let alone provide for a solution to the problem. As can be seen above, *Garrison* does not teach or even mention a denial of service attack or any other type of attack intended to consume resources of the server to cause a denial of service in this or any other section of the reference .

The Examiner also cites to *Garrison* at Figure 4A which illustrates:

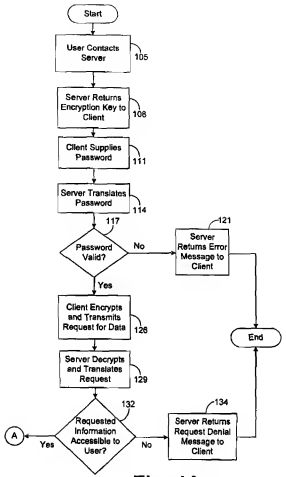

Fig. 4A

Here, *Garrison* illustrates receiving a client password, determining if the client password is valid, and determining if requested information is accessible to the user. Thus, *Garrison* **provides access to authorized users through a system that asks the user initially for a password**, then uses a server to translate the user password into an alias password, and communicates this alias password to the user. *Garrison* is only concerned with authenticating a client password to determine access to requested information. *Garrison* is completely unconcerned with denial of service attacks. As discussed above, *Garrison* does not even mention denial of service attacks, detecting an occurrence of a denial of service attack, or responding to a denial of service attack.

Garrison seems to operate under the assumption that a single password will be received from a user and a single validation process will be required to determine if the requested information is accessible to the user. *Garrison* does not address or even mention the problem of receiving invalid credentials from an attacker attempting to consume a server's resources and cause a denial of service

event. In contradistinction, the present invention in claim 1 blocks connections from the client to the first server data processing system in response to detecting a denial of service attack in which the client sends invalid credentials to the server to consume resources of the server. Thus, *Garrison* does not anticipate the claimed invention, because *Garrison* does not disclose blocking connections from the client to a first server data processing system in response to detecting the occurrence of a denial of service attack from the client, as is claimed in claim 1.

Therefore, *Garrison* is totally devoid of any teachings that disclose "responsive to detecting the occurrence of the denial of service attack, blocking connections from the client to the first server data processing system," as is claimed in amended claim 1. Consequently, under the standards of *In re Bond*, *Garrison* does not anticipate claim 1.

I.B. Garrison Fails to Disclose the Features of Replaying an Instance of the Denial of Service Attack to a Second Server Data Processing System and Sending a Command to the Second Server Data Processing System to Block Connections From the Client Responsive to A Failure of the Instance of the Denial of Service Attack on the Second Server Data Processing System

Garrison fails to anticipate claim 1, because *Garrison* does not disclose all the features taught in claim 1. In rejecting claim 1, the Examiner cites to Figure 4A which is shown above. As discussed above, the flowchart discloses validating a password. However, neither the cited portion nor any other portion of *Garrison* teaches the further step of replaying an instance of a denial of service attack, as is recited in amended claim 1.

Amended claim 1 teaches a method for responding to a denial of service attack that comprises sending invalid credentials to a server in order to consume resources of the server. *Garrison* does not disclose the steps of **replaying an instance of the denial of service attack** to *a second server data processing system* or to any other system. In addition, *Garrison* fails to disclose **sending a command to the second server data processing system to block connections from the client in response to a failure of the instance of the denial of service attack on the second server data processing system**, which is a feature taught by amended claim 1. Thus, *Garrison* fails to anticipate amended claim 1 because *Garrison* does not teach each and every feature of claim 1.

I.C. Independent Claims 9, 16, and 23

Amended independent claims 9, 16, and 23 recite features similar to those presented in claim 1. Therefore, claims 9, 16, and 23 are distinguishable over *Garrison* for at least the reasons set forth above with regard to claim 1.

I.D. Dependent Claims 2-8, 10-15, and 17-22

Claims 2-8, 10-15, and 17-22 depend on independent claims 1, 9, 16, and 23. Therefore, at least by virtue of their dependence on claims 1,9,16, and 23, *Garrison* does not anticipate these claims. In addition, dependent claims 2-8, 10-15, and 17-22 recited additional combinations of features not taught by the cited art.

For example, dependent claim 6 recites "wherein the denial of service attack from the client is occurring in response to receiving the invalid credentials includes: determining whether a number of the invalid credentials received from the client has exceeded a threshold selected to trigger a presence of the denial of service attack." Dependent claim 6 discloses that in order to determine whether a denial of service attack is occurring, a number of invalid credentials received from a client has to exceed a threshold to trigger the presence of a denial of service attack. As discussed above with regard to claim 1, *Garrison* does not mention a denial of service attack, preventing a server from being attacked by a client, or exceeding a threshold in order to determine the occurrence of a denial of service attack. Thus, *Garrison* fails to disclose the features of claim 6.

As shown above, *Garrison* is devoid of disclosure of all the features as recited in claims 1-23. Therefore, the rejection of claims 1-23 under 35 U.S.C. §102(b) has been overcome.

II. 35 U.S.C. § 103: Asserted Obviousness

The Examiner rejected claims 2, 3, 6, 10, 11, 14, 17, 18 and 21 under 35 U.S.C. § 103(a) as obvious over *Garrison* as applied to claims 1, 5, 9, 13, 16 and 20, and further in view of the Examiner taking official notice. This rejection is respectfully traversed.

The Examiner states:

> **As per claims 2, 3, 10, 11, 17 and 18**, Garrison does not specifically disclose the features of these claims. The Examiner, however, takes official notice that these elements are well known in the art of security systems. It would have been obvious to anyone having an ordinary level of skill in the art at the time the invention was made to have included these features in the invention of Garrison since they comprise very well known elements necessary for the entire system to function in a secure and controlled environment.
>
> **As per claims 6, 14 and 21**, Garrison does not disclose the features of these claims. The Examiner, however, takes further official notice that these elements are well known in the art of security systems. It would have been obvious to anyone having an ordinary level of skill in the art at the time the invention was made to have included these features in the invention of Garrison for the same reasons as stated above.

Office Action dated June 26, 2007, p. 2-3

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior

art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). The prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In determining obviousness, the scope and content of the prior art are... determined; differences between the prior art and the claims at issue are... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or non-obviousness of the subject matter is determined. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.* (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)).

II.A. No Rational Technical Underpinning Exists to Combine or Modify the References to Achieve the Present Invention Exists in the Prior Art

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *See KSR Int'l. Co. v. Teleflex, Inc.,* No. 04-1350 (U.S. Apr. 30, 2007)(citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)). The prior art must teach all of the features of the claimed invention The Examiner has admitted, and Applicants agree, that the cited prior art references fail to teach each and every feature in claims 2, 3, 6, 10, 11, 14, 17, 18, and 21. The Examiner believes these features are well known in the art of security systems. However, Applicants respectfully submit that *Garrison* fails to teach each and every feature of claims 1, 9, 16, and 23. As discussed above with regard to claim 1, great differences exist between *Garrison* and the invention in claims 1, 9, 16, and 23. Moreover, the elements that are well known in the art of security systems fails to make up for the deficiencies of *Garrison* because of the great differences between *Garrison* and the invention claims in claims 2, 3, 6, 10, 11, 14, 17, 18 and 21.

A person of ordinary skill would not be motivated to combine *Garrison* and the features noted in claims 2, 3, 6, 10, 11, 14, 17, 18 and 21 because *Garrison* is completely irrelevant to the problems associated with denial of service attacks. *Garrison* is concerned only with problems associated with providing access to authorized users through a system that asks the user initially for a password, then uses a server to translate the user password into an alias password, and communicates this alias

password to the user. Thus, due to the great differences between *Garrison* and the invention in claims 2, 3, 6, 10, 11, 14, 17, 18 and 21, it would not have been obvious to one of ordinary skill in the art to modify *Garrison* in the manner suggested by the Examiner.

The Examiner also provides no other articulated reason from any prior art to support modifying the features in *Garrison* to reach the invention in claims 2, 3, 6, 10, 11, 14, 17, 18 and 21. Instead, the Examiner relies on "official notice". If the Examiner cannot make a showing from the prior art that making all the necessary modifications to the reference teachings to achieve the present invention would be desirable, then the Examiner has simply relied on hindsight with the benefit of Applicants' disclosure to develop an incentive for the changes, which in fact, would not be obvious to one of ordinary skill in the art at the time the invention was made.

Therefore, Applicants respectfully request that the Examiner cite the prior art references, if there are any, that Examiner is basing the rejection under, as under MPEP § 2144.03. If, on the other hand, the Examiner is basing the rejection on facts within the Examiner's own personal knowledge, Applicants respectfully request that the Examiner comply with 37 CFR § 1.104(d)(2) and provide support for the Examiner's argument in the form of an affidavit "subject to contradiction or explanation by the affidavits of the applicant or other persons." Otherwise, the Examiner has failed to meet the *prima facie* burden of proving obviousness, and claims 1-23 should be allowed.

II.B. The Examiner Failed To State a Proper Reason To Combine the References Under the Standards of *KSR Int'l.*

The Examiner admits and Applicants agree that *Garrison* does not disclose the features of 2, 3, 6, 10, 11, 14, 17, 18, and 21. The Examiner asserts, however, that it would obvious to modify *Garrison* to include the additional features of claims 2, 3, 6, 10, 11, 14, 17, 18, and 21 and thereby achieve the present invention. However, the Examiner failed to state a *prima facie* obviousness rejection against claim 2, 3,6,10, 11, 14, 17, 18, and 21 because the Examiner failed to state a proper reason to combine the references under the standards of *KSR Int'l.* Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)).

Regarding a reason to combine the references, the Examiner states that, "it would have been obvious to anyone having an ordinary level of skill in the art at the time the invention was made to have included these features in the invention of *Garrison* since they comprise very well known elements necessary for the entire system to function in a secure and controlled environment." This reason does not provide a rational technical underpinning to support the legal conclusion of obviousness of claims 2,

3,6,10, 11, 14, 17, 18, and 21 in view of the combination of the Examiner's Official notice and *Garrison* considered as a whole. As a first matter, as shown above, *Garrison* does not teach a method for responding to a denial of service attack from a client. In fact, *Garrison* is devoid of **any** of the features as taught in claim 1. However, *Garrison* fails to teach or even mention detecting attacks involving sending invalid credentials to consumer server resources or responding to such an attack. Instead, *Garrison* is concerned with a method to for providing access to authorized users through a system that asks the user initially for a password, then uses a server to translate the user password into an alias password, and communicates this alias password to the user. *Garrison* does not deal with the problem at hand in the claimed invention in claims 2, 3, 6, 10, 11, 14, 17, 18, and 21. The mere fact that *Garrison* discloses a method for securing a data base processor does not make *Garrison* equivalent to the claimed invention in claims 2, 3, 6, 10, 11, 14, 17, 18, and 21. The Examiner has failed to provide a rational technical underpinning to support the legal conclusion of obviousness, as required by *KSR Int'l.* Accordingly, under standards of *KSR Int'l.*, the Examiner failed to state a prima facie obviousness rejection against claims 2, 3, 6, 10, 11, 14, 17, 18, and 21.

II.C. Garrison Teaches Away from the Presently Claimed Invention

Garrison teaches away from the presently claimed invention where *Garrison* teaches accepting each client request to the stage of validating every client password and determining if requested information is accessible to a user every time a request and/or password is received without regard for whether a denial of service attack is taking place. Such practices could potentially lead to the occurrence of denial of service events. In contradistinction, the presently claimed invention in claims 2, 3, 6, 10, 11, 14, 17, 18, and 21 are directed towards blocking all connections from a client at a first data processing system and at a second data processing system in response to detecting a denial of service attack. Thus, *Garrison teaches* away from the presently claimed invention in claims 2, 3, 6, 10, 11, 14, 17, 18, and 21 where *Garrison* fails to detect or respond to denial of service attacks.

II.D. The Proposed Combination Fails to Teach All of the Features of the Dependent Claims at Least By Virtue of their Dependence on the Independent Claims

The obviousness rejections are predicated upon the assertions made with respect to *Garrison*. As proved above, the underlying assertions made by the Examiner regarding *Garrison*'s teachings are incorrect vis-à-vis the independent claims. Specifically, *Garrison* does not teach the feature of, "blocking connections from the client to the first server data processing system in response to detecting the occurrence of the denial of service attack from the client in which credentials are presented to the first serve data processing system by the client," as taught by independent amended claim 1. For this

reason, *Garrison* does not teach all of the features of claims 2, 3, 6,10,11,14, 17, 18, 21, at least by virtue of their dependence on the independent claims.

Additionally, *Garrison* does not teach or suggest the feature of, "replaying an instance of the denial of service attack to a second server data processing system and sending a command to the second server data processing system to block connections from the client responsive to a failure of the instance of the denial of service attack on the second server data processing system," as taught by independent claim 1. Instead, *Garrison* is directed towards disclosing a method for providing access to authorized users through a system that asks the user initially for a password, then uses a server to translate the user password into an alias password, and communicates this alias password to the user. *Garrison* is wholly unrelated to the inventions of the independent claims and, accordingly, is wholly unrelated to claims 2, 3, 6,10,11,14, 17, 18, 21.

As shown above *Garrison* does not teach or suggest all of the features of claims 2, 3 ,6, 10, 11, 14, 17, 18, and 21, at least by virtue of their dependency on the corresponding independent claims. Therefore, the proposed combination and modification of the cited references when considered together as a whole does not teach or suggest all of the features of these claims. For this reason, the Examiner has failed to state a *prima facie* obviousness rejection against these claims.

III. Conclusion

The subject application is patentable over the cited references and should now be in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: September 25, 2007

Respectfully submitted,

/Mari Stewart/

Mari Stewart
Reg. No. 50,359
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants